Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A system that facilitates extracting data in connection with spam processing, comprising:

a processing unit; and

a memory for storing computer-executable instructions that when executed by the processing unit executes:

~~a computer readable storage medium comprising:~~

a component that receives a message and extracts a set of features associated with some part, content or content type of a message; and

an analysis component that examines

(1) consecutiveness of characters within a subject line of the message, wherein the analysis component establishes ranges of consecutive, repeating characters, the ranges corresponding to varying degrees of spaminess, whereby messages can be sorted by their respective individual count of consecutive repeating characters and,

(2) a content type of the message for spam in connection with building a filter, wherein the content type describes a type of data contained within a body of the message, the content type being case-sensitive and comprising a primary content-type, a secondary-content type, or a combination thereof, the primary content-type and the secondary-content type comprising at least one of a text, a multipart, a message, an image, an audio, a video, or an application, wherein the

analysis component compares the content type of the message to stored content types of a plurality of other messages to facilitate determining whether the message is spam.

2. (Original) The system of claim 1, the analysis component determines frequency of consecutive repeating characters within the subject line of the message.

3. (Original) The system of claim 2, the characters comprise letters, numbers, or punctuation.

4. (Original) The system of claim 1, the analysis component determines the frequency of white space characters within the subject line of the message.

5. (Previously Presented) The system of claim 1, the analysis component determines distance between at least one alpha-numeric character and a blob, wherein the blob comprises a random sequence of characters, numbers, punctuation, or a combination thereof.

6. (Original) The system of claim 1, the analysis component determines a maximum number of consecutive, repeating characters and stores this information.

7- 11. (Canceled)

12. (Original) The system of claim 1, the analysis component further determines time stamps associated with the message.

13. (Previously Presented) The system of claim 12, the analysis component determines a delta between time stamps.

14. (Original) The system of claim 13, the delta is between a first and a last time stamp.

15. (Original) The system of claim 1, the analysis component determines at least one of: a percentage of white space to non-white space in the subject line of the message and a percentage of non-white space and non-numeric characters that are not letters in the subject line of the message.

16. (Original) The system of claim 1, the filter being a spam filter.

17. (Original) The system of claim 1, the filter being a parental control filter.

18. (Original) The system of claim 1, further comprising a machine learning system component that employs at least a subset of extracted features to learn at least one of spam and non-spam.

19-41. (Canceled)

42. (Previously Presented) A method for evaluating spam as a function of message content, comprising:

employing a processor executing computer readable instructions stored on a computer readable storage medium to implement the following:

parsing a message to extract a set of features associated with a part, content, or content type of the message, wherein the content type describes the type of data contained within a body of the message, the content type being case-

sensitive and comprising a primary content-type, a secondary content-type, or a combination thereof;

examining the extracted set of features to identify a frequency of consecutiveness of repeating characters within a subject line of the message and to identify a distance of white-space characters between at least one alpha-numeric character and a blob comprising a random sequence of characters, numbers, punctuation, or a combination thereof to classify the message as spam or not spam;

establishing ranges of consecutive, repeating characters, the ranges correspond to various degrees of spaminess, wherein each range comprises a number range of frequencies of the consecutive, repeating characters within the subject line of the message;

employing the ranges to sort the message by the frequency of consecutive repeating characters within the subject line of the message; and

processing the message as a function of the classification.

43. (Currently Amended) The method of claim 42, ~~examining the consecutiveness of repeating characters comprises determining a frequency of the consecutiveness of repeating characters,~~ wherein the repeating characters comprise letters, numbers, punctuation, or white space.

44. (Canceled)

45. (Canceled)

46. (Previously Presented) The method of claim 42, further comprising comparing the set of features of the message to stored content types of a plurality of other message to determine whether the message is spam.

47. (Currently Amended) One or more computer-readable storage media having computer-executable instructions embodied thereon that, when executed, perform a method for facilitating extracting data in connection with spam processing, comprising:

receiving a message;

determining a particular portion of a body of the message to analyze;

extracting a set of features associated with some part, content or content type of the message;

examining consecutiveness of characters within a subject line of the message and identifying a distance comprising a number of white-space characters between at least one alpha-numeric character and a blob comprising a random sequence of characters, numbers, punctuation, or a combination thereof;

examining a content type of the message for spam in connection with building a filter, wherein the content type describes data contained within the [[a]] body of the message, the content type being case-sensitive to capture a variation of a primary content-type, a secondary-content type, or a combination thereof, each of the primary content-type and the secondary-content type comprising one of a text, a multipart, a message, an image, an audio, a video, or an application;

determining a percentage of white space to non-white space in the message and a percentage of non-white space and nonnumeric characters that are not letters in the message;

calculating a delivery time for the message using a first timestamp associated with origination of the message and a second timestamp associated with receipt of the message; and

categorizing the delivery time into one of a plurality of ranges comprising a range of amounts of time for delivering messages, the ranges corresponding to various degrees of spaminess.